International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 4, Issue 2, Apr 2014, 1-4

INFORMATION PERIMETER SECURITY OF THE ORGANIZATION

ZHANGISINA G. D[1] & SHAIKHANOVA A. K[2]

[1]Professor, Department of Head, Information Security, Kazakh National Technical University Named after K. I. Satpayev, Almaty, Kazakhstan

[2]Kazakh National Technical University Named after K. I. Satpayev, Almaty, Kazakhstan

ABSTRACT

The article describes basic technologies of defense of perimeter of the informative system as a mandatory member of the system of informative safety of organization. The necessity of introduction of the multilevel system of defense of information is shown.

The article describes the basic technologies ofprotection of information systems perimeter as a mandatory element of information security of organization. The necessity of introducing multi-level system of data protection is shown.

KEYWORDS: Information Security, Network Security, Server, Attack, Firewall, Scalable Infrastructure, Quality Monitoring, Multi, Level System

INTRODUCTION

The number of incidents related to information security, according to the leading analytical agencies is increasing. Those responsible for the information security noted increasing activity outside intruders using the latest developments in the attack, trying to penetrate corporate networks to carry out their "black" cases. They are not limited only by theft of information or deducing network nodes fail. In many cases the compromised network where used to carry out new attacks. Therefore, the protection of the perimeter of the information system is a mandatory element of the organization's information security.

Perimeter Protection Components

What components should be to protect the perimeter, minimal (basic) level of information security? To answer this question is required an analysis of the most common threats to the information resources of the organization:

- Network attacks against the unavailability of information resources (for example, Web-servers, e-mail services, etc.) - Class DoS attacks and DDoS;
- Compromise of information resources and the escalation of privileges - from both insiders and external attackers, both to the use of your resources and to cause harm;
- The actions of malicious code (viruses, worms, Trojans, spyware, etc.);
- Leakage of confidential information and data theft - as through a network (e-mail, FTP, web and etc), as well as through external media.
- Various network attacks on the application.

To minimize the security threats is need the implementation of multi-level data protection.

The Necessity to Protect the Information Perimeter

Protection of the information perimeter in needed:

- For-profit organizations that are connected to public networks;
- Governmental organizations that are connected to the Internet;
- Geographically distributed organizations;
- Communication operators;
- Financial and credit institutions.

The first level of information security that blocks hackers unauthorized access to the corporate network is a firewall. There are various manufacturers of firewalls designed to protect both small and large geographically distributed information systems.

Depending on the technology of information processing in an organization, firewalls (perimeter protection devices) are available in different models and provide different functionality, including:

- Differentiation and access control, perform user authentication, IP-address translation (NAT);
- Organization of demilitarized zones;
- Construction of various types of VPN (IPSec and SSL VPN, including decision certified by Kazakhstan needs);
- The functional control of content. Analysis of application traffic, protect traffic from viruses and various types of spyware and malware, anti-spam, URL-filtering, anti-phishing, etc.;
- The functional detection and prevention of network attacks and unauthorized network activity;
- High availability and clustering;
- Load balancing;
- Quality of Service (QoS);
- Mechanisms for user authentication;
- Integration with various systems of authentication and authorization (RADIUS, TACACS +, LDAP, and others);
- Manage access control lists routers;
- A number of other features.

The basic functionality is the distinction firewalls and access control, address translation, and topology hiding your computer network from the outside world. However, it should be noted that firewalls mainly performs filtering and traffic analysis in the third and fourth levels of the model OSI, and only a limited - at higher levels.

Another extremely important functional of firewall is the organization of demilitarized zones. This is specially protected network segments to which secure access organized from the external network (Internet) and be advised to install the server, communicating with external networks - WEB, mail, DNS, etc.

However, the firewall itself can be a target for attackers - as well as the other components of your network, from

application servers and Web-based e-mail servers to hosts and databases. To monitor and control the attacks and unauthorized network activity is recommended to use specialized products network intrusion detection and intrusion prevention (IDS/IPS). These systems allow you to track and record attempts unauthorized network activity, and optionally block attacks in real time. Best use of the data received from the sensors (servers) attack detection and the firewall attacks (on reflection of attacks) allow the use of information security monitoring. The monitoring system allows the IS to reduce all the information security events and incidents in a single console, perform intelligent analysis of attacks and their effects, and enables administrators to develop countermeasures. In addition, the monitoring system IS performs the registration and storage of information security events, which makes it possible to use the resulting material as evidence when the incident investigations and court proceedings.

The Effectiveness of the Basic Elements of Perimeter Defense

Thus, the basic elements of perimeter defense - is firewalls (and VPN-server), intrusion detection and prevention of network attacks and information security monitoring system. However, in practice, these systems are often not sufficient for effective protection against today's threats; they provide a necessary but not a sufficient level of security of information systems. *There are a number of threats, and there are more and more, from which these remedies are ineffective. These threats include:*

- Penetration of worms, viruses and other malicious code via e-mail, web-surfing, etc. Typically, this infection is not determined by a firewall running on the third level of the model OSI, or intrusion detection systems. After all, no attack, for example, when the file transfer is not performed;
- Infecting computers running over crypto tunnel (eg. within the SSL-connection to an infected web-server or IPSec-connection with contaminated network);
- That exploit unknown vulnerabilities of some applications.

For these and other reasons, for protection of corporate information systems not enough only firewall (and intrusion detection systems). Depending on the specific features of the protected system and the requirements for the level of security, it is recommended to use other systems and methods of protection. It is important to organize an effective defense at the hosts (servers and workstations, network), control of content on the network perimeter, control of leakage of confidential information, and to take some other action.

CONCLUSIONS

So, the perimeter protection of computer networks using firewalls and intrusion detection is a basic and necessity to protection of the perimeter of the information system from attacks by malicious users, a kind of "pre-filter".

The use of these technologies provides:

- Control and limit access at the perimeter;
- If necessary, authenticate users;
- Hiding the topology and the internal organization of your computer network, this greatly complicates the task of intruders.
- Organization of internal users secure access to external networks and vice versa - external network users to protect internal resources;

- Timely prevention, detection and blocking most of the attacks targeting resources information system;
- A significant increase in the efficiency of the personnel responsible for the security, cost savings arising from the inefficiency;
- Scalable infrastructure, information security corporate network;
- Centralized management of means of protection, at different parts of the corporate network (including remote locations);
- Quality monitoring and analysis of security events, facilitating the work of specialists to develop a response.

REFERENCES

1. Shangin V.G. Protection of information in computer systems and networks. - DMK-Press, 2012, 592 p.
2. Domarev V.V. Safety of information technology. A systematic approach. / V.V. Domarev - K.: Software Ltd. TTI Dia, 2004. -992 P.
3. Zegzhda D.P. Fundamentals of Information Systems Security / D.P. Zegzhda, A.M. Ivashko – M.: Goryachaya Liniya- Telecom, 2000, - 452 P.
4. Kuril A. P, Zefirov S.L., Golovanov V. B. Information security audit. - BDC-Press, 2006. – 304 P.
5. Rzhavsky K.V. Information security: practical protection of information technology and telecommunications systems: the manual. - Volgograd. Publishing house of the Volga, 2010-122P.
6. A.A. Bezbog. Methods and tools for protection of computer information: a training manual. / A. A. Bezbogov, AV Yakovlev, V. N. Shamkin. - Tambov: TSTU Press, 2006, 196P.
7. Zaitsev A.P., Shelupanov A.A., Meshcheryakov R.V. Technical means and methods of information security: Textbook for universities. - Moscow LLC "Publishing Engineering", 2009 -508 p.